Planning for Research and Development

The national security, economic prosperity, and social well being of the United States depend upon the reliable operation of a complex system of interdependent infrastructures. Energy is the lifeblood of this system. Currently, the energy infrastructure is vulnerable to disruption from physical and cyber threats. These threats are compounded by interdependencies, which amplify the consequences of a disturbance in one system and can potentially cause cascading effects across multiple infrastructures. Assuring the reliable operation of the energy infrastructure in a cost-effective manner will require new technology to prevent, detect, mitigate, and recovery from energy disruptions.

DOE works with DHS, other Federal agencies, States, local governments, and the private sector to coordinate protection activities and cultivate collaborative partnerships to assure the secure and reliable operation of the Nation's energy infrastructure. The DOE R&D program is conducted in direct support of Homeland Security Presidential Directives, as well as The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets and The National Strategy to Secure Cyberspace.

HSPD-7 designates DOE as the Federal agency with primary responsibility for facilitating the protection of critical infrastructures and key assets in the energy sector, including the production, refining, storage and distribution of oil and gas, and electric power except for commercial nuclear power facilities. HSPD-8 establishes how Federal agencies will prepare for responding to disasters and incidents, and requires that DOE provide Federal preparedness assistance to state and local governments and support efforts to ensure that first responders are prepared to respond to major events. The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets calls directly upon DOE to establish R&D strategies for the energy industry in concert with DHS and industry. In addition, The National Strategy to Secure Cyberspace calls directly upon DOE to develop best practices and new technology to increase security of PCS/SCADA systems in concert with DHS and industry. In order to fulfill these mandates, DOE, in partnership with the private sector and Federal, and state and local governments, will develop a comprehensive R&D program that improves the robustness, security, and reliability of the energy infrastructure.

The strategy of the RTD&A (Research, Technology Development, and Application**)** Program is to:

- Identify critical nodes for the energy infrastructure. Determine the causes and consequences of infrastructure outages, including interdependencies and cascading effects.

- Develop and demonstrate optimized protection, detection, mitigation, and response strategies and technologies for all physical, cyber, and natural threats.

- Provide advanced capabilities for understanding energy infrastructure operation, vulnerabilities, interdependencies, system complexities, and cascading effects.

- Deploy monitoring and display capability to assess the real-time status of the energy infrastructure for use in training and recovery operations.

Since the 1990s, numerous studies on the vulnerability and reliability of the Nation's energy infrastructure have been conducted by groups such as the President's Commission on Critical Infrastructure Protection (PCCIP), NERC, and the National Petroleum Council (NPC). Since 9/11, additional studies, such as those conducted by the National Research Council and RAND, examined vulnerabilities and R&D needs of the energy sector in the new threat environment. In total, over 100 studies of the energy infrastructure have been completed that provide a wealth of information and recommendations on steps that should be taken to make the energy infrastructure more secure.

While these studies have identified comprehensive and far-reaching R&D recommendations, they have mainly been compiled by the research communities without input from the private sector. Currently, about 85% of energy assets are owned by private companies that develop, build, operate, maintain, and protect the major portion of our energy systems. Coordinated efforts by the private sector, state and local governments, the Federal government, and the private sector will be required to reduce system vulnerabilities and mitigate the impacts of system failures. Technology providers in the private sector, academia, and our national labs will all need to play a role in a developing and implementing a comprehensive, coordinated R&D strategy.

In partnership with the private sector, DOE, as the energy sector specific lead agency, will execute this strategy by:

- Engaging our stakeholders, including DHS, other agencies, states, private industry, National Laboratories, and academia, and broadening our partnerships to leverage our limited resources.

- Developing a shared vision of a secure, reliable and robust energy infrastructure and the goals to achieve it.

- Developing roadmaps to meet the goals in our shared vision.

- Developing and demonstrating tools and technologies that improve the physical and cyber security of energy sector assets.

  - Because of the urgency of the threat, emphasize the support of tools and technologies that yield near term responses to high risk vulnerabilities.
  - Because resources are limited, support activities (particularly near term activities) that have the potential of achieving a positive return on investment.
  - Because the nature of threats and vulnerabilities is continually changing, support intermediate and long range R&D identified in the roadmaps.

- Using quantitative metrics to measure progress and accomplishments.

A. Sector Technology Requirements

One of the central principles our national homeland security policy is that homeland security is a shared responsibility among Federal, state, and local governments, the private sector, and citizens. With an estimated 85% of the nation's infrastructure owned and operated by the private sector, it is imperative that infrastructure protection and information sharing be approached as a public-private partnership that brings together the special resources and capabilities of each sector for mutual benefit.

The energy sector will use public-private partnerships to bring together the strengths of business and government to solve increasingly complex and difficult infrastructure security problems. DOE will include its industry partners in each phase of the technology development process, including planning, collaborative research and development, and implementation. The process takes advantage of the inherent relationship between homeland security and sound business practices, using market drivers to help focus scarce resources where they can effect the greatest improvements in infrastructure protection. The scope and scale of today's technological challenges require the technical skills of a wide variety of science bases. The financial challenges are equally daunting, requiring large amounts of capital for research, development, scale-up, demonstration, commercialization, and dissemination. Partnerships help to meet these technical and financial challenges by reducing the cost and risk of projects to stimulate private investment.

Visions and Roadmaps are used as a means to engage industry and other stakeholders in defining their long-term goals, technology challenges, and research priorities. These documents provide critical planning inputs for government programs. DOE helps facilitate the vision and roadmap process and analyzes the resulting technology needs to identify synergies with national infrastructure priorities.

Energy sector technology requirements will be developed, in collaboration with our stakeholders and partners, using visions and roadmaps. Through structured and facilitated sessions, participants in this process describe the current state, the desired state, and the actions needed to get from one to the other. During this process, data from prior gap analyses and analyses of other roadmaps and program plans will be examined. An up to date gap analysis will be generated. This process will provide DOE with the data necessary to perform a prioritization. Requirements, gaps, and priorities will be mapped onto DHS – OSTP Theme Areas as required and communicated to appropriate offices.

B. Current R&D Initiatives

A National Laboratory Coordinating Council (LCC) has been established. The LCC has produced an inventory of current capabilities and performed a gap analysis. It has also evaluated of existing programs and roadmaps, and defined concepts for infrastructure assurance.

Five new technologies have been or are being demonstrated as a result of a solicitation issued in 2003. They are:

- Secure encryption and authentication for SCADA systems – Retrofitable
- Train-the-Trainer Program for Low-Cost Vulnerability Assessment Tool
- Wireless Sensing System To Detect Breaches In Refinery Storage Tanks
- Advanced Surveillance System
- Visualization, Modeling, and Simulation Tool for Electrical Networks

The development of national SCADA test bed infrastructure has been initiated. Attack mechanisms and exploitation plans have been developed; secure SCADA architectures are being designed; and vendor designs are being benchmarked.

Advanced modeling, simulation and visualization tools including models for indications and warnings, flow, storage, and distribution are being developed.

A solicitation for advanced concepts that are demonstrable within two years and have the potential for a positive return on investment is in process.

C. Gaps

Key RTD&A areas include:

- Physical security – Technologies that reduce the vulnerability of energy assets to physical disruptions and attacks. Examples include access control technologies, materials hardening of facilities and equipment, advanced electric transformers, adaptive transmission grids, advanced pipeline technology, and energy storage and delivery technologies. Within this subset of requirements, the common aspects involve a very large body of work being planned by the USACE-ERDC, the DoD CIP organization and others on hardening of facilities in both a physical and cyber sense. The remaining activities are largely unique to the energy sector and its special expertise and the mature relationship between government and industry concerning this subset.

- Cyber security – Technologies that reduce the vulnerability of energy assets to cyber disruptions and attacks. Examples include secure SCADA systems, encryption/authentication protocols, and smart controls. Within this subset of requirements, the common aspects cross almost every infrastructure of this nation with the result that every major cyber R&D effort inside government and outside in industry is focused on these issues. There is tremendous opportunity for shared resources and collective knowledge with even the intelligence community providing strong efforts is NSA, ARDA and ITIC. A number of organizations are addressing the serious issues of securing existing SCADA systems, computer operating systems and applications as well as groups like DARPA and NSF looking at next generation variants of these from their very foundations to build inherently secure new generations. New encryption technology including those involving quantum methods are already being tested by industry and are expected to advance quickly, but research on countermeasures across all government and intelligence agencies will become critical before such technologies are widely released.

- Monitoring and control – Technologies that improve the ability to monitor energy operations and detect emerging threats. Examples include advanced disruptions and intrusion detection systems and real-time monitoring and control of energy assets. In this subset of requirements, the common aspects are as numerous as there are specific themes such as intrusion detection and real-time monitoring directly and by simulation of implications being pursued across a number of agencies including several DOE labs. Because of the maturity in the energy industries in the use of these systems, it would be expected that the energy sector would be a leader in such efforts.

- Modeling, simulation, and interdependencies – Technologies and methods to improve our understanding, operation, and response to vulnerabilities and disruptions within energy systems and related infrastructures, such as telecommunications, transportation, banking and finance, healthcare and water. Examples include tools for consequence analysis, modeling interdependencies, estimating repair and restoration time and cost, and simulation exercises. There are needs that cross all sectors, agencies and many industries. Several DOE labs are making substantial progress in cross sector interdependency simulations. These efforts, when combined with those in DoD and other organizations and shared with industry, and state and local government will create formidable decision support and planning systems for leaders and responders.

- Vulnerability and risk assessment – Technologies and methods for identifying physical and cyber vulnerabilities in energy assets and infrastructures and tools that help estimate risk potential; tools and methodologies that support development of a risk-based investment strategy for energy sector assets. Examples include screening methods and risk assessment and management tools that support risk informed decision making. The National CIP R&D plan shares these concerns with all sectors and their respective agencies and industries. The investment, insurance, liability perspectives of terrorism imbued into American laws and practical limitations will require much time and effort and the technologies and methods in these requirements will have many groups working to develop a broad understanding. With seats of expertise like the RAM efforts of Sandia and the maturity of the energy sector in terms of knowledge about its assets, one would again expect this sector effort to provide leadership in these issues along with DHS.

- Emergency planning, response, and recovery – Technologies and actions to improve the ability to plan for, respond to, and recover from energy emergencies. Examples include self-healing components, domestic capability to provide critical technologies, and improved response/recovery planning tools. This subset of requirements includes elements from several of the primary National CIP R&D themes including Response, Recovery and Reconstitution and the self-healing systems focus area of the Advanced Infrastructure Architectures and System Designs theme. There are very unique issues such as nuclear plants and storage facilities and the special problems of dealing with future distributed energy systems that will require this sector's attention, but there will be many opportunities within all levels of government and industry to address these fundamental requirements

While we anticipate the many of the above areas will be identified during the road-mapping process, the new DOE process contains the following features that will lead to better integration of research efforts with the National CIP R&D initiatives.

- The current Laboratory Coordinating Council will be broadened to include representatives from other Federal R&D organizations and will meet periodically with state, local, and industry energy sector partners.

- Roadmaps will be used as basis for solicitations.

- DOE will use the output of the annual CIP R&D plan required by HSPD-7 to create and update our roadmaps.

- As a major stakeholder, DHS will be involved with both the road-mapping process and the solicitations. The roadmaps generated should yield areas of interest for DHS as well as DOE support.

D. Planned R & D Initiatives

DOE will work with DHS and other Federal R & D organizations to encourage R & D to improve the protection of the energy infrastructure. DOE is closely involved with current efforts, led by OSTP to develop the infrastructure protection R & D plan, which will identify initiatives.

Current Technology Projects

ENERGY ASSURANCE TECHNOLOGIES

Project Fact Sheet

National Supervisory Control and Data Acquisition (SCADA) Test Bed

INCREASING ENERGY RELIABILITY BY IMPROVING THE SECURITY OF SCADA SYSTEMS

While U.S. energy systems are considered the most robust and reliable in the world, their vulnerability has now been recognized. As these systems have become increasingly dependent on powerful, electronic communications tools, the Internet, and supervisory control and data acquisition (SCADA) systems, cyber attacks have become an increasing threat.

SCADA systems are computer-based systems that monitor and control remote devices that manage commodity flows within the power grid and pipelines. Historically, SCADA systems were designed for reliability and operability, with little emphasis on security. These systems have evolved from isolated centrally controlled mainframe-based architectures using proprietary communication paths, to modern distributed networks with more potential for public access using Internet technology and common operating systems. These trends have been accelerated by deregulation, and use of common standards and interconnections between utilities.

The DOE Office of Energy Assurance (OEA) has launched a multi-laboratory partnership to implement the National SCADA Test Bed (NSTB) to test control system vulnerabilities and security hardware and software. *The National Strategy to Secure Cyberspace* calls on DOE, in cooperation with the Department of Homeland Security, other federal agencies, and the private sector, to develop best practices and new technology to increase security of distributed control and SCADA systems. The NSTB will identify SCADA vulnerabilities and recommend security standards to protect critical energy infrastructure SCADA systems. By teaming with industry, the NSTB will become a full-scale infrastructure suite of facilities for testing and validating industry control systems. Jointly run by Sandia National Laboratories and the Idaho National Engineering and Environmental Laboratory, the NSTB will integrate the critical infrastructure protection strengths of several other DOE National Laboratories including Argonne National Laboratory (oil and gas infrastructure) and Pacific Northwest National Laboratory (electricity infrastructure).

Benefits

- Apply current technologies for mitigating existing vulnerabilities.
- Establish fully functional and diverse alliances with energy, standards, and vendor communities.
- Contribute to security guidelines based on emerging threats.
- Train industry to perform self-assessments of systems to improve security.
- Provide a focal point for energy sector protection activities in vulnerability reduction and system reliability.
- Design and develop future architectures and technologies that increase system robustness against attack and enable self-healing of the infrastructures.

Applications

The NSTB will provide capabilities to address the utility industry's SCADA vulnerability concerns including automation and networking equipment found throughout the utility.

Project Partners

Sandia National Laboratories

Idaho National Engineering and Environmental Laboratory

Argonne National Laboratory

Pacific Northwest National Laboratory

U.S. Department of Energy

Interested in Participation or Additional Information About the National SCADA Test Bed, Contact:

Juan Torres
SCADA Program Manager
Sandia National Laboratories
P.O. Box 5800
Albuquerque, NM 87185
Phone: 505-845-9804
E-mail: jjtorre@sandia.gov

Julio Rodriguez
Manager, Critical Infrastructure Assurance
Idaho National Engineering and Environmental Laboratory
P.O. Box 1625
Idaho Falls, ID 83415-3840
Phone: 208-526-2039
E-mail: ju2@inel.gov

For Program Information, Contact:

Hank Kenchington
Technology Manager
U.S. Department of Energy
Office of Energy Assurance
1000 Independence Ave., SW
Washington D.C. 20585
Phone: 202-586-1878
Email:
henry.kenchington@hq.doe.gov

Project Description

The NSTB provides a national program to secure the energy SCADA communications and control infrastructure. The program includes six mission areas to provide capability that will evolve from developing attack detection and prevention technologies for existing SCADA systems into a national effort to improve the security of the next-generation architectures and technology advances. The six areas of focus are as follows:

- Demonstrate energy sector vulnerabilities to industry through testing and demonstration of credible threats to the private sector, to raise awareness and develop industry acceptance of the need for improved levels of security, both physical and cyber.
- Conduct vulnerability assessments of SCADA systems to raise the awareness of equipment suppliers and utilities, and collaborate to provide near-term solutions and long-term best practice solutions into the program.
- Address disruptions in electricity, oil and gas services, and interdependent infrastructures that may require immediate and long-term remedial actions by the government and energy industries.
- Develop, with industry, technologies that provide electricity, oil and gas systems, and infrastructures that are inherently secure and dependable for their users.
- Develop risk mitigation strategies for current SCADA systems, and develop next-generation architectures for intelligent, secure infrastructures.
- Support the development of national standards and guidelines for secure SCADA design and implementation, and help align international interests with national needs by participating in development of requirements and standards.

Through laboratory partnering, the NSTB brings unique and extensive capabilities that can be leveraged to support the DOE energy assurance mission. The NSTB provides personnel with comprehensive SCADA system technical expertise and industry relationships; availability of SCADA systems, facilities, and infrastructure assets that represent real-world systems' network resources and connectivity; red teaming and assessment expertise; modeling and simulation resources; cryptography and information security capability; research and standards development support; and other SCADA-related test bed and security programs.

Progress and Milestones

- Establish a business portal for doing business with industry and government agencies. (4Q/04)
- Develop an industry liaison group charter. (4Q/04)
- Assess industry training needs related to SCADA security. (4Q/04)
- Identify applicable standards and regulatory bodies. (4Q/04)
- Issue test reports on SCADA system testing. (1Q/05)
- Establish National SCADA Test Bed VPN Network between SNL and INEEL. (4Q/04)

Economics and Commercial Potential

A disruption in the energy infrastructure can impact the security of the nation and the well-being of our citizens. Improvements in the robustness of the energy infrastructure can substantially mitigate such losses as well as address emerging cyber treats. The government, private sector (e.g., energy utilities), and general public demand a more robust and secure energy infrastructure. Such demands will, by necessity, provide significant economic and commercial opportunities.

ENERGY ASSURANCE TECHNOLOGIES

Project Fact Sheet

Advanced Sensor System for Energy Infrastructure Assurance

Benefits

- A combined shock and hydrocarbon sensor maximizes detection of possible events such as impacts resulting in a sudden release of hydrocarbons and other transients
- Wireless communication links eliminate the need for hard wired sensors and their associated installation and maintenance costs
- Remote monitoring minimizes response time to detected events and potentially reduces the need for routine human monitoring
- Sensors with on-board power (battery integrated with a renewable power source) and low power consumption requires infrequent operator intervention
- Continuous computerized monitoring increases assurance of the monitored energy assets

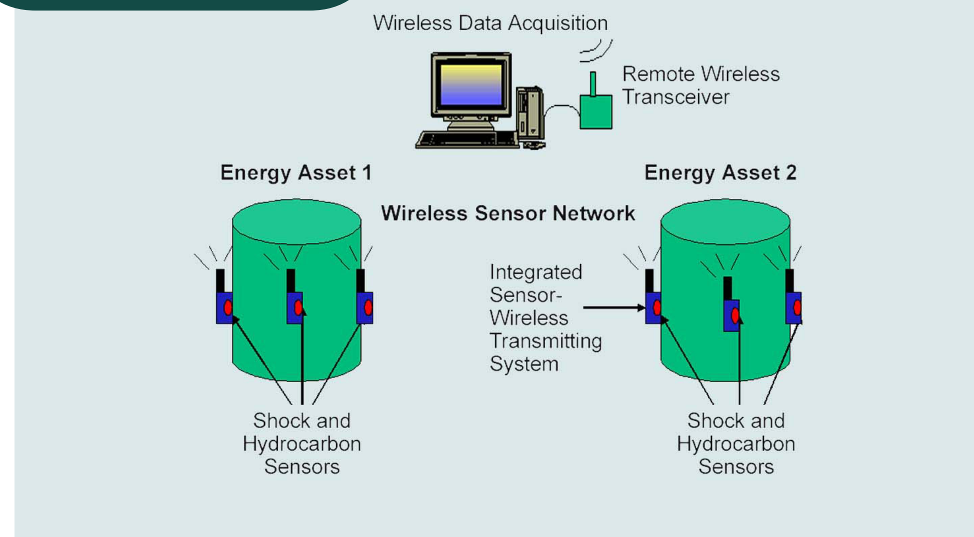
Applications

The integrated wireless sensing system will be designed to detect severe shocks and leaks of hydrocarbons as a result of breaches caused by high energy impacts and to alert facility personnel. This system can be installed in any facility that contains substantial amounts of hydrocarbons, particularly in storage tanks, where early detection of a leak is important. This includes refineries, gasoline, heating oil, and diesel storage facilities and energy infrastructure transport facilities. Since the wireless system is designed to be modular, it is anticipated that it will be easily adaptable to other sensing applications by replacing the sensor modules. This should also make the concept valuable to sensing applications in other industries, such as the chemical industry, where rapid detection of leaks at storage or process facilities is a high priority.

An integrated wireless sensor system will enable remote continuous monitoring of energy storage facilities to detect breaches from various causes

Significant quantities of energy assets including heating oil, diesel fuel, and gasoline are stored and transported within the United States and constitute a vital part of the energy infrastructure. Energy asset storage tanks are potentially vulnerable to malicious acts from a remote location with potential serious consequences including fire, explosion, environmental damage, potential loss of life, and economic losses due to release of materials and damage to infrastructure. This project addresses development and demonstration of a wireless sensor technology that aids in the early detection of damage due to such an act. Prompt detection will enable a rapid response, mitigate the adverse impact of such an event, and, hence, aid in protecting the U.S. energy infrastructure.

The project approach to developing this system involves integration of a shock sensor and a hydrocarbon sensor with a wireless communication system, and an on-board power source rechargeable through solar power. The best and most appropriate technology for each of these components will be chosen from those available commercially or from those under development at Oak Ridge National Laboratory (ORNL).


Wireless Data Acquisition
Remote Wireless Transceiver
Energy Asset 1
Energy Asset 2
Wireless Sensor Network
Integrated Sensor-Wireless Transmitting System
Shock and Hydrocarbon Sensors
Shock and Hydrocarbon Sensors

The unique sensor technology enables remote early detection of energy asset (e.g. storage tank) breaches by wireless transmission of sensor data from each asset to a remote central location

Project Description

The project will develop and demonstrate a sensor system that would enable early detection of hydrocarbon leaks from breaches to the energy infrastructure, thereby minimizing the operational and economic consequences of such events.

Specifically, the project will develop and demonstrate a wireless sensing system to detect a breach in storage tanks. The sensing system works by detecting both an impact through a shock sensor and by measuring hydrocarbon levels in the vicinity of the tank. The measured hydrocarbon levels are then compared with average levels for that location. If abnormal levels are detected, this information will then be transmitted on a real time basis to a remote operator (such as in a control room) who could respond rapidly to minimize potential losses and consequential damage to personnel and property. The project will initially focus on examining the feasibility of developing a system that can be rapidly deployed in energy storage tank locations using commercially available technologies for shock sensing, hydrocarbon sensing, and wireless communications. Technologies developed at ORNL for sensing and sensor wireless communications will be utilized if demanded by the sensitivity and range requirements for the application.

Progress and Milestones

This project includes the following milestones:

- Survey available shock and hydrocarbon sensors, along with commercially available wireless technologies (2Q/04)
- Down-select initial shock and hydrocarbon sensors from those commercially available and from those developed at ORNL with laboratory verified performance to meet project goals (4Q/04)
- Modify and initiate field-testing of transmitter and receiver systems for wireless monitoring of the down-selected sensors (3Q/04)
- Complete assembly and initiate first field-testing of the combined wireless shock and hydrocarbon sensor system (2Q/05)
- Complete system validation and testing by conducting a system demonstration at an appropriate energy sector facility (4Q/05)

Economics and Commercial Potential

The economic value of storage tanks for petroleum products in the U.S. is very significant. An API survey conducted in 1989 estimated the total number of such tanks in the U.S. at 700,000, inclusive of refining, marketing, transportation, and production. These storage tanks represented a capital asset of about $700 billion and more than 2 billion barrels of energy-related materials, with an estimated value of over $60 billion. Prompt detection of adverse events impacting these assets will not only result in direct economic benefits through minimizing loss of materials and damage to the infrastructure, but will also prevent indirect losses through loss of productivity.

Although hydrocarbon sensors are currently used in storage facilities, these are hard-wired sensors. The sensor technology being developed in this project has a significant market potential since it represents state-of-the art in shock and hydrocarbon detection. In addition, it will be wireless-enabled with a renewable power source that can be charged through solar power. It is anticipated that the advantages inherent in the system being developed will result in substantial commercial benefits through replacement of existing sensors and through incorporation into future installations. The complete sensor system will be commercialized through project partner(s) already actively involved in the industrial sensors sector.

Project Partners

Oak Ridge National Laboratory
Oak Ridge, TN

Pegasus Technologies, Inc.
Lenoir City, TN

Konarka Technologies, Inc.
Lowell, MA

Delphian Corporation
Northvale, NJ

Materials Technology Institute
St. Louis, MO

Interested in joining the partnership, being informed of outcomes, or being a demonstration site? Contact:

Vinod K. Sikka
Group Leader, Materials Processing
Oak Ridge National Laboratory
Bldg. 4508, MS-6083
Bethel Valley Road
Oak Ridge, TN 37831-6083
Phone: 856-574-5112
FAX: 865-574-4357
Email: sikkavk@ornl.gov

or

David Szucs
U.S. Department of Energy
National Energy Technology Laboratory
626 Cochrans Mill Road
Pittsburgh, PA 15236-0940
Phone: 412-386-4899
Email: szucs@netl.doe.gov

For Program Information, Contact:

Mike Soboroff
Program Manager
U.S. Department of Energy
Office of Energy Assurance
1000 Independence Ave, SW
Washington, DC 20585
Phone: 202-586-4936
Email: Mike.Soboroff@hq.doe.gov

or

Albert B. Yost II
Business Area Coordinator
U.S. Department of Energy
National Energy Technology Laboratory
3610 Collins Ferry Road
Morgantown, WV 26507-0880
Phone: 304-285-4479
Email: ayost@netl.doe.gov

For Additional Information:

Visit our home page at
www.ea.doe.gov

Office of Energy Assurance
U.S. Department of Energy
Washington, D.C. 20585

January 2004

ENERGY ASSURANCE TECHNOLOGIES

Project Fact Sheet

Critical Infrastructure Test Range

Benefits

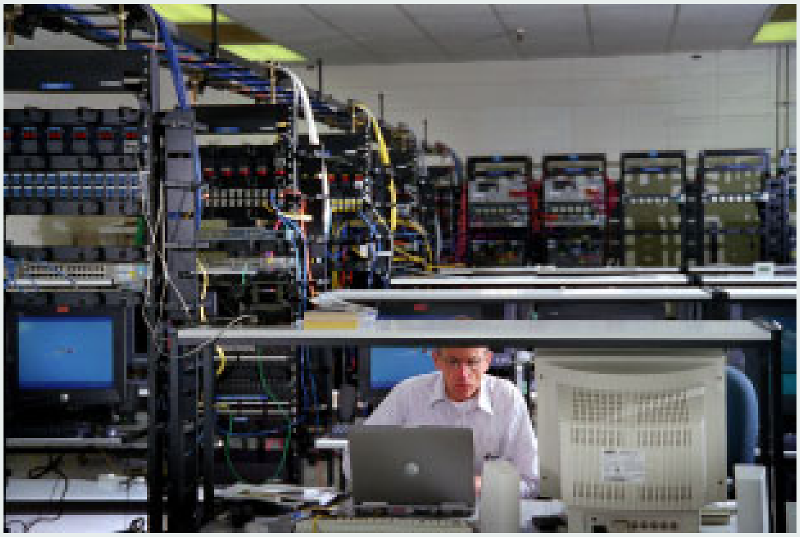
- Helps identify vulnerabilities in critical energy infrastructure
- Provides "quick fixes" as well as improved designs for more secure and robust systems and components
- Leads to developing and implementing protective measures
- Leads to development of better systems standards and certification
- Used for vulnerability awareness education for industry and other stakeholders

Applications

The Test Range is used to independently identify energy assurance system and component vulnerabilities, assess these vulnerabilities and then develop, verify and validate solutions. PCS vendors and end-users can then use these solutions for their systems. We can then apply the knowledge gained to the development of national and commercial standards and certification procedures for energy assurance-related systems and components. This will ensure that new systems and components integrated into the existing infrastructures do not introduce new vulnerabilities.

Helping protect the nation's energy infrastructure by providing component and system-level testing

The Idaho National Engineering and Environmental Laboratory (INEEL) Critical Infrastructure Test Range consists of specialized and integrated test beds and test control centers. The test range is located on the 890-square-mile U.S. Department of Energy reservation, located in southeastern Idaho. The INEEL Critical Infrastructure Test Range includes capabilities to test a variety of process control systems (PCS) – including those using supervisory control and data acquisition (SCADA[1]), distributed control systems (DCS) and programmable logic controllers (PLC) – cyber security, communications and electrical power grid in an integrated manner and at full scale. Oil and gas delivery systems can be tested in cooperation with DOE's Rocky Mountain Oilfield Testing Center (RMOTC).



An engineer monitors one of many ongoing tests at the Cyber Security/SCADA Test bed. These Test beds are two elements of the INEEL Critical Infrastructure Test Range, which provides system-level testing capability to test the nation's critical infrastructure systems and protective measures at near full scale.

[1] Supports the National SCADA Test Bed Program, jointly run by INEEL and Sandia National Laboratory

Project Description

The Test Range provides a component and system-level testing capability to test the nation's critical infrastructure systems and protective measures at near full scale. This approach will allow our nation to fix the vulnerabilities facing us today, use that information to develop defensive procedures for today's infrastructures, and develop tomorrow's smart infrastructures that will be much more attack resistant by design and construction.

The CI Test Range consists of specialized critical infrastructure test beds and test control centers. These individual test beds can also be integrated to test interdependencies. The principal programmatic components are as follows:

- SCADA
- Cyber Security
- Communications
- Power Grid
- Physical Security

Progress and Milestones

- Established two industry agreements established with SCADA manufacturers. (1Q/04)
- Installed one commercial SCADA system for testing. (1Q/04)
- Commercial SCADA system testing. (3Q/04)
- Install new Land Mobile Radio (LMR) components to support emergency responder communications. (3Q/04)
- International SCADA Conference. (4Q/04)
- Facility modifications to expand SCADA and Cyber Test Beds capabilities. (3Q/04)

Economics and Commercial Potential

A disruption in the energy infrastructure can impact the security of the nation and well being of our citizens. As a result of the August 14, 2003 power outage in the northeast United States and Canada, 50 million people were impacted and an estimated $4.5-$12B in economic activity was lost. Improvements in the robustness of the energy infrastructure can substantially mitigate such losses.

The Government, private sector (e.g., energy utilities) and general public are demanding a more robust and secure energy infrastructure. Such demands will, by necessity, provide significant commercial opportunities.

Project Partners

Bechtel Telecommunications

AT&T Wireless

Siemens

ABB Inc. – Network Management

U.S. Department of Energy

U.S. Department of Homeland Security

U.S. Department of Defense

Interested in joining the partnership, being informed of outcomes, or being a demonstration site? Contact:

Alan Snyder
Program Manager
Idaho National Engineering and
Environmental Laboratory
P.O. Box 1625
Idaho Falls, ID 83415-3840
Phone: 208-526-1725
Email: amq@inel.gov

or

Jacqueline Gernant
Project Manager
Idaho Operations Office
Idaho Falls, ID 83415-3840
Phone: 208-526-1742
Email: gernanja@id.doe.gov

For Program Information, Contact:

David Salem
Technology Manager
U.S. Department of Energy
Office of Energy Assurance
1000 Independence Ave, SW
Washington, DC 20585
Phone: 202-586-8710
Email: David.Salem@hq.doe.gov

For Additional Information:

Visit our home page at
www.ea.doe.gov

Office of Energy Assurance
U.S. Department of Energy
Washington, D.C. 20585

March 2004

ENERGY ASSURANCE TECHNOLOGIES

Project Fact Sheet

Cyber Security for Utility Operations

Benefits

- Develops fundamental tools needed to identify, authorize and validate the source of data or access to data on SCADA systems
- Provides key management tailored to needs of SCADA systems
- Provides cryptographic security in SCADA retrofit solutions
- Provides secure authentication of maintenance ports
- Supports a future embedded solution for new Intelligent Electronic Devices

Applications

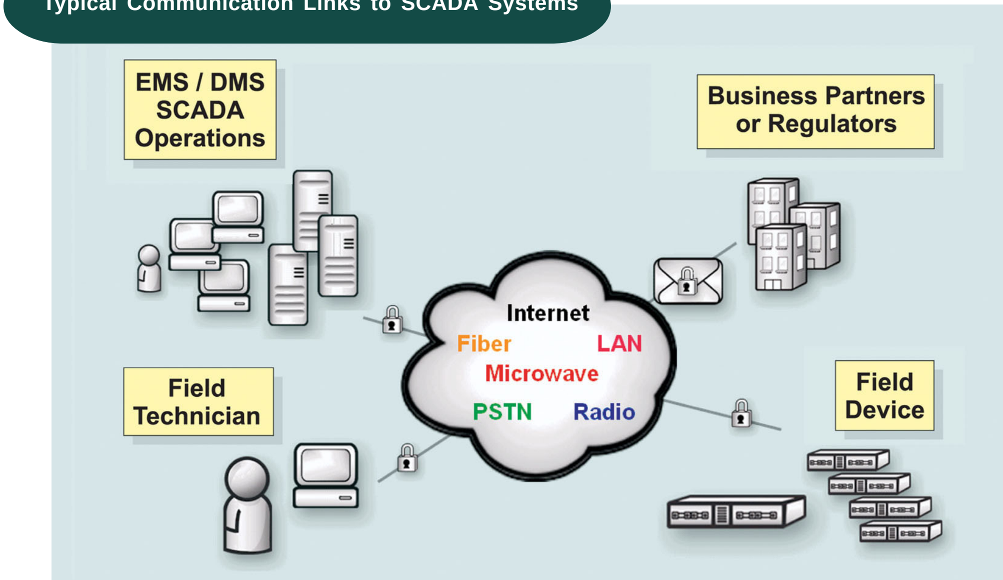
The critical technology components developed and demonstrated by this project will advance a comprehensive, rather than a piecemeal, solution to SCADA system security and provide a solution that will be more efficient and cost effective. The nearer term applications will be retrofit solutions to legacy SCADA systems in the utility industry, including electric, natural gas, water and waste water utilities. Longer term, the project work will advance the development of new hardware and software designs for new SCADA systems and components, such as embedded solutions for Intelligent Electronic Devices, for these same industries. These solutions could also be applied to any SCADA system, regardless of industry, that has numerous communication links, field devices, and users.

Advanced cryptographic techniques will be integrated into encryption, authentication, and key management products to provide comprehensive, cost effective cyber security

The utility industry increasingly relies upon Supervisory Control and Data Acquisition (SCADA) systems and Energy Management Systems (EMS) in the performance of utility operations. Initial SCADA and EMS systems operated in closed communication loops accessible only by their utility owners. Security protocols were not then deemed necessary. However, increasingly these systems now use the same public telecommunications switching networks and the Internet available to the public for SCADA and EMS systems communications. Generally, these SCADA and EMS resources were designed with minimal security features to protect against cyber intrusions and details of these security features are usually obtainable in the public domain. This situation makes many critical energy infrastructure SCADA systems potentially vulnerable to cyber intrusion. Retrofit solutions for many older legacy SCADA systems are often hampered by inherent system limitations. No comprehensive cost effective cyber security solution currently exists. This project seeks to advance the achievement of such a solution.

Recent cryptography R&D has enabled advances in algorithms, hardware designs, and key management for efficient, low-power authentication and encryption. These results will be integrated with the project industrial partners' initial cryptographic system level design. A proof-of concept design for SCADA critical technology components will be developed and will then be demonstrated at the facilities of a project utility partner.

Typical Communication Links to SCADA Systems



This project will advance SCADA cyber security for utilities by integrating advanced cryptographic techniques into new products to cost effectively protect SCADA communication links.

Project Description

The project will identify and integrate into a system design the critical technologies that must be demonstrated to move towards commercializing products needed for comprehensive and cost effective cyber assurance of SCADA systems. The project focuses on developing technology to provide retrofit solutions for existing legacy SCADA systems that will protect against unauthorized access to the system from the "outside" via SCADA communication links. The technology needed to protect "data at rest" (who has access to the data, how they can use the data, and the controlled time of its use) is well understood and accepted. Requirements to deploy a cost effective solution to protect the "data in transit" is also well understood. Implementation, however, is dependent on a low cost design for three components:

- A secure authentication module is needed to strengthen the access control to device maintenance ports.
- A secure encryption and authentication module is needed to protect data over installed SCADA and EMS communication links.
- A secure management system is needed for key management and distribution.

The project will bring technologies from Sandia together with those from its industry partners to develop these components sufficiently to perform a proof-of-concept demonstration.

Progress and Milestones

This project includes the following milestones:

- Evaluate and update current utility security requirements (1Q/04 [completed])
- Assess and update the project partner's cyber security system designs (2Q/04)
- Integrate state-of-the-art products from Sandia, TecSec, and Mykotronx into a system design (2Q/04)
- Demonstrate a proof-of-concept security system at utility facilities (3Q/04)
- Refine commercialization plan for a cyber security system (3Q/04)

Economic and Commercial Potential

There are over one thousand SCADA systems in operation in electric utilities, each with many remote terminal units (RTUs). Electric utility SCADA systems typically are larger and more complex than in other utilities. A large electric utility can have about 200 communication links and 5,000 RTUs associated with their SCADA system. There are also many SCADA systems in service in other segments of the nation's utility infrastructure (e.g., natural gas, water and waste water utilities). All are candidates for the retrofit solutions being developed in this project.

The economic costs of retrofitting an existing SCADA system with additional cyber security measures must be weighed against the potential losses that can be caused by a successful malicious cyber attack against the system and its perceived likelihood. These losses can include not only disruptions to internal utility operations, but also disruption of service to its customers and, in extreme cases, disruption to the economic activity of a local area or a region. Generally, the utility industry acknowledges that SCADA systems have some vulnerabilities to cyber intrusions. However, the cost and difficulty in implementing additional security measures, particularly for older SCADA systems, is dissuading utilities from making upgrades. Without a more comprehensive and relatively lower cost solution, most utilities are unlikely to embark on a security upgrade to their SCADA systems. By advancing a comprehensive low cost solution, this project can make the business case for SCADA system security upgrades more compelling and, thereby, contribute towards improving the assurance of the U.S. energy infrastructure.

Project Partners

Sandia National Laboratories
Albuquerque, NM

Mykotronx, Inc.
Torrance, CA

TecSec, Inc.
Vienna, VA

OPUS Publishing
Seal Beach, CA

Peoples Energy
Chicago, IL

DTE Energy
Detroit, MI

Interested in joining the partnership, being informed of outcomes, or being a demonstration site? Contact:

Timothy J. Draelos, Ph.D.
Cryptography & Information Systems Surety Department
Sandia National Laboratories
P.O. Box 5800; MS 0785
Albuquerque, NM 87185-0785
Phone/Fax: (505) 844-8698 / 845-7065
Email: tjdrael@sandia.gov

or

David Szucs
U.S. Department of Energy
National Energy Technology Laboratory
626 Cochrans Mill Road
Pittsburgh, PA 15236-0940
Phone: 412-386-4899
Email: szucs@netl.doe.gov

For Program Information, Contact:

Craig Zingman
Program Manager
U.S. Department of Energy
Office of Energy Assurance
1000 Independence Ave, SW
Washington, DC 20585
Phone: 202-586-1043
Email: Craig.Zingman@hq.doe.gov

or

Albert B. Yost II
Business Area Coordinator
U.S. Department of Energy
National Energy Technology Laboratory
3610 Collins Ferry Road
Morgantown, WV 26507-0880
Phone: 304-285-4479
Email: ayost@netl.doe.gov

For Additional Information:

Visit our home page at
www.ea.doe.gov

Office of Energy Assurance
U.S. Department of Energy
Washington, D.C. 20585

March 2004

ENERGY ASSURANCE TECHNOLOGIES

Project Fact Sheet

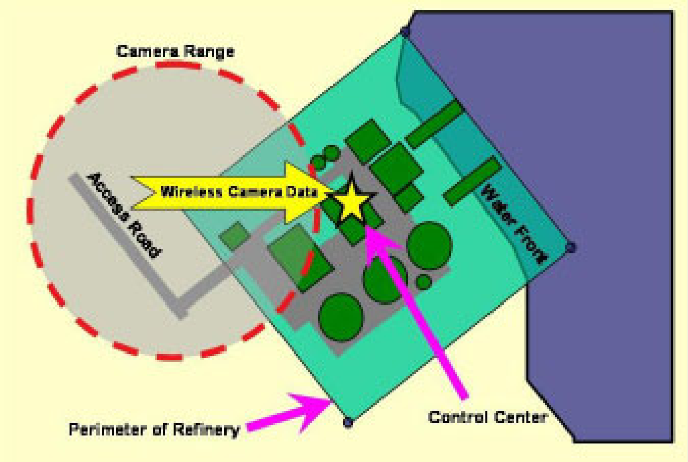
REFINERY AWARENESS SECURITY SYSTEM (RASS)

ADVANCED NETWORK SENSORS AND VIDEO PROVIDE LINK TO EARLY WARNING CRISIS MANAGEMENT SYSTEM FOR ECONOMICALLY ENHANCING PREVENTION AND MITIGATION CAPABILITIES

Refineries share a common security concern in providing continuous, comprehensive and cost effective site security. Their expansive facility boundaries that must be monitored and protected present a security challenge. Inadequately protected areas are potentially vulnerable to a wide range of intrusions that could jeopardize facility operation, expensive and difficult-to-replace equipment, and personnel. Existing monitoring systems and patrols typically employed by refineries for security purposes may not be able to effectively cover the entire facility boundary continuously and are costly to maintain. The use of advanced sensor and video technology, such as RASS, can improve the effectiveness of security, while potentially reducing associated operational costs.

The RASS protection approach uses a surveillance camera system with infrared, robotic high-resolution, and thermal imaging devices to spot an "exception" to ordinary behavior. The robotic camera then "locks on" to the moving object after alerting the Control Center staff through visual and audible alarms. The technology is used in conjunction with a Concept of Operations that includes an integrated response with local law enforcement.

Graphic Representation of RASS Concept



The RASS collects and analyzes surveillance data to automatically alert security of site intrusions. It is scalable to monitor all, or part, of site boundaries, as desired.

BENEFITS

- Can continuously monitor entire facility boundary with very low false alarm rate
- Lower operating costs vs. current stand-alone security systems and patrols
- Features high detection sensitivity
- Provides a complete emergency management system, including integration with law enforcement
- Open architecture system with lower cost than proprietary systems now available

APPLICATIONS

In addition to refineries, any energy facility (oil, natural gas or electricity) that has a vulnerability to illegal entry across its boundary coupled with the possibility of significant physical or economic damage resulting from such an intrusion is a candidate for the technology. This technology is also well suited for facilities in the chemical and transportation industries that possess these characteristics. The RASS technology is itself an extension of the PROTECT program, initiated by DOE, which mitigates the impact of chemical attacks on high-threat interior infrastructures, such as subways, airports, and buildings. The PROTECT system is already operational in the Washington, DC, subway and is being installed at a Boston inter-modal facility.

Project Description

The project will demonstrate enhanced energy facility security by leveraging currently developed and demonstrated DOE technologies. Security will be enhanced in a cost-effective manner, leading to lower operational costs when compared with current stand-alone security systems and patrols.

Numerous sensor systems — and a variety of camera systems — available in today's market are capable of intrusion detection, including seismic and motion detection. These systems, however, often do not meet industry needs because of high initial costs, high maintenance costs, unreliability due to false alarms or lack of robustness, and, frequently, proprietary software. Many systems, initially developed for the military, are very expensive and do not fit well in the civilian environment, where there is a very low tolerance for false alarms and the need for a system that does not require a highly trained technician.

The RASS program offers a level of sensitivity needed to identify intrusions using site specific software to distinguish routine activities from unwanted intrusions. The fixed cameras operate 24/7 and are equipped with software that, once an exception is identified, activates a robotic camera that follows the intruding person or vehicle. The system is scalable for protecting areas of greatly varying sizes and adaptable to other energy facilities. The RASS technology will be demonstrated at the Trainer, PA refinery of ConocoPhillips, Inc.

Progress and Milestones

This project includes the following milestones:

- Site Survey and Preliminary Design Customized to Demonstration Facility (1Q/04 [complete])
- Engineering and Network Design (2Q/04)
- Command and Control Software Design and Testing (3Q/04)
- Integration and Installation of RASS (4Q/04)
- Final Testing and Training of Demonstration Facility Staff (4Q/04)
- Technology Demonstration and Transfer (1Q/05)

Economic and Commercial Potential

The economic consequences of a major security breach at a refinery can be significant. It can lead to a shutdown of the facility resulting in loss of its economic value for months or longer to the facility owner and may require costly repairs. Additionally, it could potentially result in significant negative price and supply impacts to consumers of refined petroleum products. Use of the RASS at petroleum refineries will safeguard against security breaches and, thereby, minimize the possibility of economic losses to the facility owner and to petroleum consumers.

In addition, the use of this technology can reduce the need for costly security patrols. With the addition of RASS technology, larger areas of the refinery boundary could be monitored, while utilizing fewer security personnel for the task. Therefore, the annual security operating costs when using this new technology could be less than the costs of using the patrols alone. The potential offered by RASS to provide an enhanced level of security, and energy assurance, without increasing the facility's security related operational costs should be an attractive option for corporate and facility security decision makers to consider as a method to better manage corporate risk.

Project Partners

Argonne National Laboratory
Argonne, IL

LiveWave, Inc.
Newport, RI

ConocoPhillips, Inc.
Houston, TX

Interested in joining the partnership, being informed of outcomes, or being a demonstration site? Contact:

Anthony J. Policastro
Argonne National Laboratory
9700 South Cass Avenue (Bldg 900)
Argonne, IL 60439
Phone: 630-252-3235
Email: policastro@anl.gov

or

David Szucs
U.S. Department of Energy
National Energy Technology Laboratory
626 Cochrans Mill Road
Pittsburgh, PA 15236-0940
Phone: 412-386-4899
Email: szucs@netl.doe.gov

For Program Information, Contact:

David Salem
Technology Manager
U.S. Department of Energy
Office of Energy Assurance
1000 Independence Ave, SW
Washington, DC 20585
Phone: 202-586-8710
Email: David.Salem@hq.doe.gov

or

Albert B. Yost II
Business Area Coordinator
U.S. Department of Energy
National Energy Technology Laboratory
3610 Collins Ferry Road
Morgantown, WV 26507-0880
Phone: 304-285-4479
Email: ayost@netl.doe.gov

For Additional Information:

Visit our home page at
www.ea.doe.gov

Office of Energy Assurance
U.S. Department of Energy
Washington, D.C. 20585

February 2004

ENERGY ASSURANCE TECHNOLOGIES

Project Fact Sheet

Risk Assessment Methodologies for Energy Infrastructures

Benefits

- Provide a systematic, risk-based approach for evaluating and improving the security of energy infrastructure networks
- Applicable to electric power transmission lines and energy pipelines and their associated critical elements and facilities
- Provide security analyses based on specific system-level vulnerabilities, threats, and consequences of an attack
- Enable identification of critical system nodes and facilities and security risks
- Provide system owners and operators with cost-benefit analyses of possible security upgrades

Applications

The proposed work will support energy infrastructure security and protection efforts by providing a systematic performance-based risk assessment approach that will enable energy customers to assess system-level risks and identify consequence mitigation strategies. This will provide customers and utilities with the ability to compare options for improvements in energy system security and reliability, including interdependencies, relative to their associated costs.

Methods and tools to identify, evaluate, and help reduce system vulnerabilities

The security and protection of our energy infrastructure is extremely important to our nation’s economy and social well-being. A major disruption to our energy infrastructure could significantly impact many segments of the population through impacts on basic human services, transportation, telecommunications, emergency services, banking, or manufacturing. Recently, intentional malevolent attacks, have become a realistic possibility that must now be considered. If carried out successfully, an attack could compromise the integrity and function of a facility or infrastructure, causing serious injuries or fatalities or leading to cascading outages and damage to other facilities or infrastructures, ultimately causing serious economic impacts. Malevolent attacks can be physical or cyber-based, coordinated and planned by either outside groups or insiders, and can include multiple, coordinated attacks against critical or important facilities. These low-probability, high-consequence events require performance-based approaches to insure facility or system security and protection. This is especially true for systems, like the U.S. energy infrastructure, that have critical elements that are highly distributed and widely dispersed.

The techniques developed to address intentional malevolent attacks and other high consequence events are often risk-based. This approach compares relative risks of an attack on the system based on the severity of the potential consequences of a given attack, the probability of the attack, the security effectiveness of the facility to the attack, and the ability to recover from the attack. These approaches have been developed and utilized in the electric power and natural gas transmission pipeline infrastructures, but have focused at the plant or company level.

Project Description

The focus of this project is to provide two major elements of the energy infrastructure – electric power generation/transmission systems and natural gas transmission pipeline systems – with improved performance-based methods and tools to identify, evaluate, and help reduce system vulnerabilities to a wide range of potential malevolent events or attacks. While there are differences between these two energy infrastructure sectors, they have many similarities including being highly dispersed systems with key facilities that are widely scattered, making them difficult to protect using only traditional physical security techniques. Additionally, these two sectors have become increasing dependent on each other. For example, many electric utilities and independent power producers utilize natural gas for electric power generation and therefore interruption of the natural gas supply could significantly impact electricity generation. In other cases, natural gas transmission pipelines utilize electric powered compressors to supply natural gas to consumers and an interruption in electric power could impact natural gas supply.

This project integrates three energy infrastructure vulnerability and risk assessment methods developed at Sandia – one for electric power transmission, one for petrochemical facilities, and one for critical asset identification in dispersed networks – into one tool for analyzing these important elements of the energy infrastructure. This approach will provide customers and utilities with a comprehensive, cost-effective, performance-based approach to assess the vulnerabilities of these energy services. This integrated risk assessment approach will enable customers and utilities to 1) identify system-level critical nodes and facilities based on various event scenarios, 2) identify and compare the risks and consequences of these events, and 3) identify cost-effective approaches to mitigate these risks and consequences and improve system security and reliability. The integrated risk assessment approach will be demonstrated and validated in cooperation with energy industry partners to pilot test the developed tools in the second year of this project. After validation, the approach will be developed into an education and training program that will be provided to industry and regulatory agencies through a train-the-trainer program developed in cooperation with industry.

Progress and Milestones

This project includes the following milestones:

- Upgrade existing risk-based vulnerability assessment methods for the electric transmission and petrochemical industries (3Q/04)
- Integrate the risk assessment methods with critical system node evaluation tool (4Q/04)
- Assess one or two energy networks in cooperation with industry participants using the developed tools to evaluate ease of use and completeness (2Q/05)
- Coordinate training program and methodology commercialization (4Q/05)

Economic and Commercial Potential

The economic consequences of a major security breach at a refinery or attack on an electric power line can be significant. It can lead to a shutdown of the energy network resulting in a loss of its economic value for extended periods, with cascading impacts throughout the economy of the region and the nation. Use of the developed risk assessment approach can help reduce vulnerabilities of energy systems and help minimize the consequences of security breeches or malevolent attacks.

In addition, the use of these techniques can help identify the critical elements of an energy network and focus protection efforts and upgrades on those facilities or elements. This enables energy system owners and operators with the ability to identify the most cost-effective methods to improve overall system security and reliability.

Project Partners

Sandia National Laboratory

Gas Technology Institute

American Gas Association

Interstate Natural Gas Association of America

Bonneville Power Authority

Tennessee Valley Authority

Interested in joining the partnership, being informed of outcomes, or being a demonstration site? Contact:

Mike Hightower
Sandia National Laboratories
P.O. Box 5800, MS0710
Albuquerque, NM 87185
Phone: 505-844-5499
Email: mmhight@sandia.gov

or

Swenam Lee
U.S. Department of Energy
National Energy Technology Laboratory
626 Cochrans Mill Road
Pittsburgh, PA 15236-0940
Phone: 412-386-4664
Email: swenam.lee@netl.doe.gov

For Program Information, Contact:

Mr. James McGlone
Program Manager
U.S. Department of Energy
Office of Energy Assurance
1000 Independence Ave, SW
Washington, DC 20585
Phone: 202-586-8710
Email: James.McGlone@hq.doe.gov

or

Mr. Albert B. Yost II
Business Area Coordinator
U.S. Department of Energy
National Energy Technology Laboratory
3610 Collins Ferry Road
Morgantown, WV 26507-0880
Phone: 304-285-4479
Email: ayost@netl.doe.gov

For Additional Information:

Visit our home page at
www.ea.doe.gov

Office of Energy Assurance
U.S. Department of Energy
Washington, D.C. 20585

February 2004

ENERGY ASSURANCE TECHNOLOGIES

Project Fact Sheet

VISUALIZATION AND SIMULATION TOOL FOR CHARACTERIZING CRITICAL AND VULNERABLE NODES IN MULTIPLE ENERGY INFRASTRUCTURE SECTORS

BENEFITS

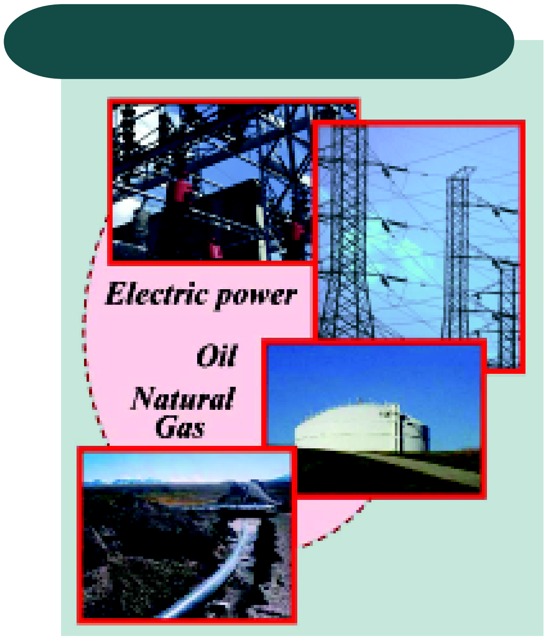
- Provide users the ability to identify an electrical network's critical assets and components
- Predict the response of the system to events
- Maps electrical components affected by outages, and visualize outage areas and affected systems.

APPLICATION

The new technology, a modeling and simulation (M&S) tool, will give end users the ability to identify an electrical network's critical nodes, predict the response of the system to events, map electrical components affected by outages, and visualize outage areas and affected systems. Specifically, the new tool will combine the power of the LANL IEISS Solver algorithms with the visualization and spatial intelligence of the General Electric (GE) Smallworld toolkit application to help plan recovery from loss of critical components.

DISRUPTION OF THE NATION'S ENERGY SYSTEM WOULD DIRECTLY AND ADVERSELY IMPACT THE ECONOMIC SECURITY OF OUR NATION.

Since the middle of the 1970s, researchers have studied energy generation and transmission networks, such as electric power grids to assist federal, state, and local agencies to understand these infrastructures, to track their evolution, to identify their strengths and weaknesses, to assess their reliability, and to analyze their economics. Much of the analysis of the electric power industry worked to identify outage events that may impact the reliable supply of electric power and the development of vulnerability mitigation options and business continuity strategies for federal decision-makers. Inherent attributes of the electricity supply system, natural causes, or man-made causes each constitute possible sources of disturbances in the power system. Detailed transmission-level utility models and teams of engineers analyzed the models using state-of-the-art power flow simulation tools to identify (i) service and outage areas, (ii) outage duration, (iii) critical system components, (iv) restoration strategies, (v) mitigation options, and (vi) system performance. The goal is to determine the electric grid's ability to supply the aggregate electrical demand and energy requirements of its customers, taking into account outages of system elements. Recently LANL has also investigated the impact of regional deregulation on system reliability: differences in state and federal guidelines or policies, differences among state deregulation policies within the same geographic region, planned new regional transmission organizations and new independent system operators create a complex new environment for the electric power industry. We envision a diversity of possible applications for analyses based on IEISS: Primarily, one can accurately identify critical components and vulnerabilities in coupled infrastructure systems, assess how future investments in the systems might affect quality of service, perform integrated cost-benefit studies, evaluate the effect of regulatory policies, and aid in decision-making during crises.



An outage in one energy system can cause failures in other systems. The new technology will give end users the ability to identify a network's critical assets and components and predict the response of the system to events.

Project Description:

This project combines the leadership and technical experience of two national laboratories, Los Alamos National Laboratory (LANL) and Idaho National Engineering and Environmental Laboratory (INEEL), with the industry leadership of General Electric (GE) in developing capability to help assure the long-term reliability and stability of the energy infrastructure. This new technology, a modeling and simulation tool, will enable end users to identify a network's critical nodes, predict the response of the system to events, map electrical components affected by outages, and visualize outage areas and infrastructure interdependencies systems. This tool will combine the power of the LANL IEISS Solver algorithms with the visualization and spatial intelligence of the General Electric Smallworld toolkit application. Development of the new analytical tool will be accomplished by combining the analytical power of the LANL IEISS Solver algorithms and the usability, and market acceptability of the General Electric (GE) Smallworld Spatial Technology application. The program will be completed and demonstrated at Ameren UE facilities in St Louis with Ameren data.

Progress and Milestones

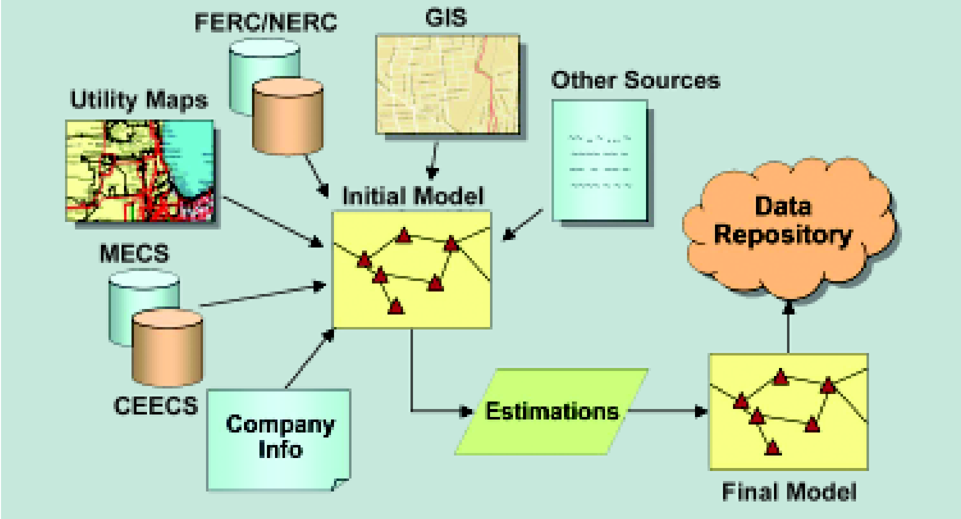
This project includes the following milestones:

- Complete design, construction and preliminary testing of the prototype model (3Q/04)
- Complete application and validation experiment at the National SCADA Testbest at the Idaho National Laboratory (4Q/04)
- Complete final demonstration of the model at the St. Louis Headquarters of Ameren UE (4Q/04)

Economic and Commercial Potential:

Upon successful demonstration of the tool, it is anticipated that GE will incorporate the tool into its product line. Potential sales are estimated at several million dollars in the first year.

The Final Model Presents Visualized Results for Utility Use



When a disruption is detected, data inputs from many sources and in a variety of formats can be combined with company information to provide impact estimates for contingency planners and decision makers.

Project Partners

Los Alamos National Laboratory

Idaho National Laboratory

General Electric Network Reliability Services

Ameren UE – Energy Delivery Technical Services

Interested in joining the partnership, being informed of outcomes, or being a demonstration site? Contact:

Steven Fernandez
Energy and Infrastructure Analysis Group, D-4
Mailstop F604
Los Alamos National Laboratory
Los Alamos, NM 87544
(505) 665-2116
Email: sjf@lanl.gov

or

Swenam Lee
U.S. Department of Energy
National Energy Technology Laboratory
626 Cochrans Mill Road
Pittsburgh, PA 15236-0940
Phone: 412-386-4664
Email: swenam.lee@netl.doe.gov

For Program Information, Contact:

James McGlone
Program Manager
U.S. Department of Energy
Office of Energy Assurance
1000 Independence Ave, SW
Washington, DC 20585
Phone: 202-586-8710
Email: James.McGlone@hq.doe.gov

or

Albert B. Yost II
Business Area Coordinator
U.S. Department of Energy
National Energy Technology Laboratory
3610 Collins Ferry Road
Morgantown, WV 26507-0880
Phone: 304-285-4479
Email: ayost@netl.doe.gov

For Additional Information:

Visit our home page at
www.ea.doe.gov

Office of Energy Assurance
U.S. Department of Energy
Washington, D.C. 20585

January 2004

OEA Makes Technology Award to Support Development of Wireless Sensor Network for Energy Asset Protection

Within the United States and throughout the world, the fundamental importance of energy systems has made these assets a potential target for terrorists. Technologies that enhance the physical security of critical energy assets are a key tool that can be employed to protect assets from malicious acts. As part of OEA's responsibilities under HSPD-7 (PDF 97 KB) the Office supports programs with the private sector to demonstrate technologies that can help ensure the reliability and security of the energy infrastructure.

In September 2004 OEA made an award to Eaton Corporation of Milwaukee, Wisconsin to develop a wireless sensor network for the physical protection of energy assets. The objective of the project is to develop a low-cost, robust, Wireless Sensor Network (WSN) to enable pervasive, real-time threat sensing, assessing, and evaluation to assure the physical security of the Nation's energy critical infrastructure. Eaton's Team Members on this project are DOE's Oak Ridge National Laboratory (ORNL) and the Electric Power Research Institute (EPRI).

Wireless sensor network technology is fundamentally transforming the architecture of physical security systems by allowing pervasive distributed sensors to be cost effectively deployed throughout the Nation's critical infrastructure. The system under development will implement a threat-aware, self-configuring wireless network with a reasoning system capable of interpreting and integrating spatially and temporally distributed, multi-spectral data and asynchronous information while postulating assertions about threats using Anticipatory theory. Anticipatory technology, modeled after a human's intuition to reason, enables the system with the capability to begin to react even before the event starts to unfold.

The project will begin in January 2005 and has a 24-month duration. During Phase 1 of the project the team will collect and analyze system requirements, develop baseline models for evaluation of performance via simulation, and refine and migrate the models into the development of prototype hardware. Phase 1 work also includes identification of sensor types required for physical security. During Phase 2 of the project the technology will be validated by conducting a series of field experiments in an end-user facility.

For more information on this project please contact Mike Soboroff, at OEA or Eaton's technical contact Jose A. Gutierrez. For more information about DOE's Oak Ridge National Laboratory and the Electric Power Research Institute Links please visit their websites.